UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICHAEL VISCARDI, individually and on behalf of all others similarly situated, *Plaintiff*, v. GOVERNMENT EMPLOYEES INSURANCE COMPANY d/b/a GEICO, GEICO CASUALTY COMPANY, and GEICO GENERAL INSURANCE COMPANY, *Defendants*.	Case No. **COMPLAINT - CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Michael Viscardi ("Plaintiff") individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendants Government Employees Insurance Company d/b/a GEICO, GEICO Casualty Company, and GEICO General Insurance Company (collectively, "GEICO" or "Defendants").

NATURE OF THE ACTION

1. Plaintiff brings this class action on behalf of himself and all other individuals ("Class Members") who had their sensitive personal identifying information—here, customers' and other consumers' highly sensitive driver's license numbers—disclosed to unauthorized third parties during a data breach compromising GEICO's online sales system (the "Data Breach").

2. GEICO writes private passenger automobile insurance policies, offering coverages to insureds in all 50 states and the District of Columbia.[1] It markets its policies mainly by direct response methods where most customers apply for coverage directly to the company via the internet or over the telephone.

[1] U.S. SEC. AND EXCH. COMM'N, FORM 10-K (Dec. 31, 2019), https://www.berkshirehathaway.com/2019ar/201910-k.pdf (last visited May 6, 2021).

3. GEICO collects vast amounts of personal information and sensitive data from prospective clients, current and former customers, and other consumers in connection with issuing insurance policies to consumers and during the insurance claims process. In order to utilize the services provided by GEICO, customers must provide sensitive personal information. For example, "during the quoting, application, or claims handling processes," GEICO obtains an individual's "Name, Address, Phone number, Social Security number, Driver's license number, Date of birth,"[2] among other sensitive personal information. On information and belief, during the insurance claims process, GEICO also requires submission of similar personal information in connection with processing claims, including from individuals who are not necessarily GEICO policyholders.

4. GEICO promises it will restrict access to nonpublic personal information to those individuals and entities who need to know that information to provide products or services.[3] It promises it will maintain "a variety of physical, electronic, and procedural safeguards to protect [its' customers] information from unauthorized access by third parties, and further promises that information "about [its] former customers and about individuals who have obtained quotes from [GEICO] is safeguarded to the same extent as information about [GEICO's] current policyholders."[4] But its efforts to protect customers' and other consumers sensitive information fall short of acceptable data security standards.

5. In a Notice of Data Breach dated April 9, 2021 (the "Notice"), GEICO informed affected victims "of an incident that affected the confidentiality" of their personal information, and that the incident occurred between November 24, 2020 and March 1, 2021. According to the Notice, unauthorized third parties accessed driver's license numbers through GEICO's online sales system and that the information "could be used to fraudulently apply for unemployment

[2] GEICO, *Privacy Policy, Geico Respects Your Privacy*, https://media.geico.com/legal/privacy_policy.htm (last visited May 6, 2021).

[3] *Id.*

[4] *Id.*

benefits" under the victims' names. The Notice further instructed those affected to review any mailings they receive from their state's unemployment agency/department and to contact the agency/department if there is any chance fraud is being committed.

6. While the Notice indicated that GEICO secured the affected website "as soon as it became aware of the issue" and that it has implemented additional security enhancement to help prevent future fraud and illegal activities on its website, unfortunately for Plaintiff and class members, the damage is already done.

7. Plaintiff Viscardi and numerous other class members received the Notice, and their sensitive driver's license numbers are already exposed to criminals. Hackers harvest driver's license numbers because they are highly valuable pieces of personal information. A driver's license can be a critical part of a fraudulent, synthetic identity, with reports indicating that the going rate for a stolen identity is about $1,200 on the dark web, and that a stolen or forged driver's license, alone, can sell for around $200.[5]

8. GEICO not only failed to provide the level of data protection that it promised, but its data privacy and security measures fell well short of acceptable industry standards, thus exposing customers' and other consumers' sensitive personal information to an increased risk of misuse by unauthorized third parties (i.e., fraud and identity theft).

9. As a result of Defendants' conduct and the resulting Data Breach, Plaintiff's and class members' privacy has been invaded, their sensitive drivers' license information is now in the hands of criminals, and they face a substantially increased risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from identity theft and fraud.

---

[5] Lee Mathews, *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach,* FORBES (Apr. 20, 2021, 11:57 A.M. EDT), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=146576a68658 (last visited May 6, 2021).

10. Plaintiff, on behalf of himself and the Class, seeks remedies, including monetary damages and injunctive relief, for GEICO's negligence, negligence per se, breach of implied contracts, invasion of privacy, and violations of New York's consumer protection law.

PARTIES

11. Plaintiff Michael Viscardi is a citizen of the state of New York and resides in Holtsville, New York. On or about April 9, 2021, GEICO sent, and Plaintiff Viscardi subsequently received, a letter to Plaintiff confirming that he was impacted by the Data Breach; that his driver's license number was exposed as part of the breach; and that fraudsters may use that stolen information in connection with applying for fraudulent unemployment benefits in his name.

12. Defendants GEICO Casualty Company, GEICO Indemnity Company, GEICO General Insurance Company, and Government Employees Insurance Company (collectively "GEICO") are Maryland corporations with their principal places of business in Chevy Chase, Maryland. GEICO is an insurance company and wholly owned subsidiary of Berkshire Hathaway, Inc., and it is authorized to conduct business in the State of New York, with corporate headquarters located at Chevy Chase, Maryland. GEICO is one of the largest auto insurance companies in the United States, boasting assets of more than $32 billion.[6]

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332 (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), is a class action involving 100 or more class members, and because Plaintiff and Defendants are citizens of different states. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

---

[6] U.S. SEC. AND EXCH. COMM'N., FORM 10-K, FORM 10-K (Dec. 31, 2019), https://www.berkshirehathaway.com/2019ar/201910-k.pdf (last visited May 6, 2021).

14. The Court has personal jurisdiction over Defendants because Defendants conduct significant business in the State of New York, thus availing themselves to New York's markets by selling auto insurance policies; have sufficient minimum contacts with the state of New York; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in New York.

15. Venue properly lies in this judicial district pursuant to 28 U.S.C. § 1391 because, *inter alia,* a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this district; Defendants transact substantial business and have agents, in this district; a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district; and because Plaintiff resides within this district.

FACTUAL ALLEGATIONS

A. GEICO Collects Vast Amounts of Sensitive Personal Information From Consumers

16. GEICO primarily offers private passenger automobile insurance to individuals in all 50 states and the District of Columbia. GEICO also insures motorcycles, all-terrain vehicles, recreational vehicles, boats and small commercial fleets and acts as an agent for other insurers who offer homeowners, renters, life and identity management insurance to individuals who desire insurance coverages other than those offered by GEICO.[7]

17. GEICO collects and stores vast amounts of personal information from prospective clients, current and former customers, and other consumers, as part of its regular business practices. Included in this information is highly sensitive driver's license numbers.

18. GEICO's marketing is primarily through direct response methods in which applications for insurance are submitted directly to the companies via the Internet or by telephone, and to a lesser extent, through captive agents.

19. Competition for private passenger automobile insurance, which is substantial, tends to focus on price and level of customer service provided. GEICO's cost-efficient direct response

[7] U.S. SEC. AND EXCH. COMM'N., FORM 10-K (Dec. 31, 2019), https://www.berkshirehathaway.com/2019ar/201910-k.pdf (last visited May 6, 2021).

marketing methods and emphasis on customer satisfaction enable it to offer competitive rates and value to its customers.

B. GEICO Promised To Protect Its Customers' and Other Consumers' Personal Information From Unauthorized Disclosures

20. GEICO recognizes the importance of keeping consumers' personal information private and repeatedly promises to keep that personal information confidential and protect it from unauthorized disclosure. For instance, the Privacy Policy appearing on GEICO's primary website states, in relevant part:

> **GEICO RESPECTS YOUR PRIVACY**
>
> Protecting your privacy is very important to us. Customers have trusted us with their insurance needs since 1936, and we take our obligation to safeguard and secure personal information very seriously. We want you to understand how we protect your privacy and when we collect, use, and share information.[8]
>
> …
>
> **CONFIDENTIALITY AND SECURITY**
>
> We restrict access to your Information to employees who we have determined need it to provide products or services to you. We train our employees to safeguard customer information, and we require them to sign confidentiality and non-disclosure agreements. We maintain a variety of physical, electronic, and procedural safeguards to protect your Information from unauthorized access by third parties.
>
> Information about our former customers and about individuals who have obtained quotes from us is safeguarded to the same extent as Information about our current policyholders.

21. GEICO recognizes the particular significance of keeping consumers' personal information obtained through its website and assured its customers transparency regarding how such information would be treated. GEICO's Internet Security Policy appearing on GEICO's primary website states:

---

[8] GEICO, *Privacy Policy, Geico Respects Your Privacy*, https://media.geico.com/legal/privacy_policy.htm (last visited May 6, 2021).

GEICO SECURES YOUR DATA

At GEICO.com, the privacy and security of customer data is as important to us as it is to you. Physical safeguards, procedural controls and data access controls protect your data from unauthorized access. We continually monitor our systems to prevent unauthorized attempts at intrusion.

OUR SECURITY

GEICO.com uses strong encryption (Transport Layer Security or TLS) for transmitting private information via the Internet. TLS uses a private key to encrypt data that is transferred over the TLS connection. This protocol is a standard used by many websites when you submit confidential information, such as credit card numbers and other personal data. TLS creates a secure connection between your browser and our server. Addresses of web pages using a TLS connection start with https: instead of http: and most browsers also display an icon of a closed padlock when you visit a page using TLS.

In addition, the Policyholder Service Center portion of our website is only available to policyholders. It provides a private and secure environment to access policy and account information.[9]

C. **The Data Breach and Its Impact**

22. In early April 2021, GEICO notified consumers that their sensitive personal information—namely, driver's license numbers—was compromised in a security breach of its online sales systems that occurred between November 24, 2020 and March 1, 2021. The Notice dated April 9, 2021 described the incident as follows:

> We recently determined that between November 24, 2020 and March 1, 2021, fraudsters used information about you – which they acquired elsewhere – to obtain unauthorized access to your driver's license number through the online sales system on our website. We have reason to believe that this information could be used to fraudulently apply for unemployment benefits in your name.[10]

[9] GEICO, *Privacy Policy, Geico Secures Your Data*, https://media.geico.com/legal/security_policy.htm (last visited May 6, 2021).

[10] Geico, *Notice of Data Breach* (Apr. 9, 2021), STATE OF CALIFORNIA DPT. OF JUSTICE, https://oag.ca.gov/system/files/DL3_IndNoticeLttr_CA_Redacted.pdf (last visited May 6, 2021).

23. Plaintiff Viscardi received a Notice from GEICO, which was sent to him on or about April 9, 2021. In the Notice, GEICO confirmed that "[t]he data obtained by the fraudsters from GEICO was limited to your driver's license number."

24. While the Notice indicates that "as soon as it became aware of the issue" GEICO "secured the affected website and worked to identify the root cause of the incident", the Notice does not provide the date of when GEICO learned of or "became aware of" the incident. Instead, the Notice merely states that GEICO "recently determined" of the incident and provides no further details.

25. The breach of GEICO's system is not unexpected. On February 16, 2021 the New York State Department of Financial Services ("DFS") issued an alert regarding an ongoing systemic and aggressive campaign to exploit security flaws in public-facing websites offering instant quotes—particularly those that offer instant online automobile insurance quotes—to steal non-public information ("NPI").[11] According to the alert, the unauthorized collection of NPI appears to be part of a growing fraud campaign targeting pandemic and unemployment benefits. DFS first became aware of the campaign when it received reports from two auto insurers in December 2020 and January 2021 that cybercriminals were targeting their websites that offer instant online automobile insurance quotes to steal unredacted driver's license numbers.

26. Insurers' instant online auto quoting websites are the primary entry point for cybercriminals to access customers' NPI. As the industry has accelerated adoption of faster-quoting processes and tools, new vulnerabilities have opened.[12] According to DFS, insurers noticed an unusually high number of abandoned quotes or quotes not pursued after the display of the estimated insurance premium. On the instant quote websites, "criminals entered valid name, any date of birth and any address information into the required fields" and "then displayed an

[11] DEPARTMENT OF FINANCIAL SERVICES, *Industry Letter* (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_edn1 (last visited May 6, 2021).

[12] *Id.*

estimated insurance premium quote along with partial or redacted consumer NPI including a driver's license number. The attackers captured the full, unredacted driver's license numbers without going any further in the process and abandoned the quote."[13]

27. In January 2021, DFS alerted approximately a dozen entities maintaining such websites that they were likely targets of hackers looking to gain access to New Yorkers' NPI, specifically driver's license numbers. Following the alert, six more insurers apparently reported to DFS the malicious targeting of their websites—two of which insurers reported that the attackers failed to gain access to NPI and four of which reported that the attackers did gain access to NPI or that their investigation was still ongoing. Neither the websites affected, nor the insurers were named in the alert.

28. The increase in interest in driver's license numbers is, in part, a product of the changes brought on by the Covid-19 pandemic, as various types of financial transactions that used to exclusively be conducted in person are transferred online. Some states are also allowing residents to use expired driver's licenses for various purposes for an extended period, due to difficulty in securing the in-person DMV appointments necessary to renew them.[14]

29. Unsurprisingly, fraudulent unemployment claims have spiked during the pandemic, as more money has become available to displaced workers and the requirements for filing have eased. Many states have paid out tens of millions of dollars to scammers, a phenomenon largely driven by the use of stolen personal information. Hackers have been caught not just using sensitive personal data for these fraudulent unemployment claims, but also hacking into existing unemployment accounts to change bank payment information.[15]

---

[13] DEPARTMENT OF FINANCIAL SERVICES, *Industry Letter* (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_edn1 (last visited May 6, 2021).

[14] CPO MAGAZINE, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited May 6, 2021).

[15] *Id.*

30. The United States Department of Labor estimates that pre-pandemic fraudulent unemployment claims accounted for about 10% of all filings.[16] A normal yearly cost for fraudulent unemployment claims is about $3 billion per year in fraud; recent reports indicate that that number ballooned to $200 billion during the pandemic. Fraudulent first-time claims drove quite a bit of this activity, but experts expect the problem to persist even as most Americans head back to work. Some will fail to notify the state unemployment office of their change in employment status, creating an opening for scammers.

31. GEICO knew or should have known that its website was a likely target of cybercriminals looking to gain access to customers' driver's license numbers in order to use that information to commit unemployment benefits fraud, among other fraud and identity theft.

32. GEICO failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumers' personal information, and failed to implement basic safeguards to protect the security, confidentiality, and integrity of that information.

D. It is Well Established That Security Breaches Lead to Identity Theft

33. The actual extent, scope and impact of the Data Breach on GEICO's customers remains uncertain. Nevertheless, the harm caused to Plaintiff and class members by the Data Breach is already apparent. Criminals now possess Plaintiff's and class members' driver's license numbers, and their only purpose is to monetize that data by selling it on the dark web or using it to commit other fraud.

34. Defendants had a duty to keep Plaintiff's and class members' personal information confidential and to protect it from unauthorized disclosures. Plaintiff and class members provided their personal information to GEICO with the understanding that it would comply with its obligations to keep such information confidential and secure from unauthorized disclosures.

---

[16] Megan DeMatteo, *Unemployment fraud costs victims $200 billion annually in the U.S. – here's how to protect yourself*, CNBC (Apr. 27, 2021), https://www.cnbc.com/select/how-to-protect-yourself-from-unemployment-fraud/ (last visited May 6, 2021).

35. Defendants' data security obligations were particularly important given the substantial increase in data breaches in recent years, which are widely known to the public and to anyone in Defendants' industry.

36. Data breaches are by no means new and they should not be unexpected. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks.

37. It is well known amongst companies that store sensitive personally identifying information that sensitive information—like driver's license numbers—is valuable and frequently targeted by criminals.

38. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

39. There may be a time lag between when sensitive personal information is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

40. With access to an individual's sensitive information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the

[17] *Id*. at 29 (emphasis added).

victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[18]

41. Sensitive personal information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs and other Personal Information directly on various illegal websites making the information publicly available, often for a price.

42. Driver's license information has become extremely valuable to identity thieves.[19] For example, a fake U.S. citizenship kit for sale: passport, SSN, driver's license and birth certificate is offered on the dark web for 0.218 bitcoin (or $1,400 at the time) and a stolen/fake driver's license (by U.S. state) for $200.[20]

43. Criminals are particularly interested in driver's license numbers because of the value attached to this data. A driver's license can be a critical part of a fraudulent, synthetic identity, with reports indicating that the going rate for a stolen identity is about $1,200 on the dark web, and that a stolen or forged driver's license, alone, can sell for around $200.[21]

---

[18] *See* FEDERAL TRADE COMMISSION, WARNING SIGNS OF IDENTITY THEFT, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 6, 2021)

[19] IDENTITY THEFT RESOURCE CENTER, *Can Someone Steal Your Identity From Your Driver's License?* https://www.idtheftcenter.org/can-someone-steal-your-identity-from-your-drivers-license/ (last visited May 6, 2021).

[20] Daniel Shkedi, *Heart of Darkness: Inside the Darknet Markets that Fuel Financial Cybercrime*, BIOCATCH, https://www.biocatch.com/blog/financial-cybercrime-darknet-markets (last visited May 6, 2021).

[21] Lee Mathews, *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach,* FORBES (Apr. 20, 2021, 11:57 A.M. EDT), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=146576a68658 (last visited May 6, 2021).

44. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Defendants failed to take reasonable steps to adequately protect GEICO's systems from being breached, leaving GEICO customers exposed to risk of fraud and identity theft.

45. Defendants were, and at all relevant times have been, aware that the sensitive personal information GEICO handles and stores in connection with its services is highly sensitive. Because GEICO is a company that provides insurance services involving highly sensitive and identifying information, Defendants were aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

46. Defendants were aware, or should have been aware, of regulatory and industry guidance regarding data security, and they were alerted to the risk associated with failing to ensure that GEICO's systems were adequately secured.

47. Defendants permitted class members' personal information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

48. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[22]

49. As a result of the events detailed herein, Plaintiff and class members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of personal information; harm resulting from damaged credit scores and information; loss of time and money preparing for and

[22] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited May 6, 2021).

resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of personal information.

50. As a result of the Data Breach, Plaintiff's and class members' privacy has been invaded, their driver's license numbers are now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

E. Plaintiff's Experience

51. Plaintiff Michael Viscardi is a citizen of New York and resides in Holtsville, New York.

52. On or around February 14, 2021, Plaintiff received a letter from the New York Department of Labor informing him that he was eligible for Pandemic Unemployment Assistance.

53. On or around February 12, 2021, Plaintiff received another letter from the New York Department of Labor notifying him of a fraudulent claim for unemployment benefits made in his name.

54. On or around April 9, 2021, GEICO sent Plaintiff a letter notifying him that his Personal Information was impacted by the Data Breach. The letter stated that "between November 24, 2020 and March 1, 20201, fraudsters used information about [Plaintiff] – which they acquired elsewhere – to obtain unauthorized access to [Plaintiff's] driver's license number through the online sales system on [GEICO's] website."

55. Plaintiff is self-employed and did not apply for unemployment benefits. Upon information and belief, Plaintiff's personal information, i.e., his driver's license number, was stolen during the Data Breach and was used to make a fraudulent claim for unemployment benefits in his name.

56. Plaintiff subsequently received a letter from his bank, informing him of an attempt to transfer funds from his joint bank account to an unauthorized account.

57. Plaintiff has taken (and continues to take) considerable precautions to protect the unauthorized dissemination of his Personal Information. To date, he has spent approximately 15 hours monitoring accounts and otherwise dealing with the fallout of the Data Breach. Unfortunately, as a result of GEICO's failure to implement its promised and paid-for security practices, Plaintiff's sensitive information was disseminated without his consent, has already been fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

58. As a result, Plaintiff suffered injury and/or damages, including but not limited to actual identity theft, time and expenses spent on credit monitoring and identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data and lost property in the form of his breached and compromised Personal Information. Additionally, as a result of the Data Breach, Plaintiff now faces a substantial risk that unauthorized third parties will misuse his Personal Information.

CLASS ALLEGATIONS

59. Plaintiff brings this action on behalf of himself and the following Classes pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> **Nationwide Class**
> All residents of the United States whose personally identifiable information was compromised in the GEICO Data Breach occurring in or around November 24, 2020 and March 1, 2021.
>
> **New York Class**
> All residents of New York whose personally identifiable information was compromised in the GEICO Data Breach occurring in or around November 24, 2020 and March 1, 2021.

60. The above defined classes are collectively referred to as the "Class" or "Classes." Plaintiff reserves the right to re-define the Class(es) prior to class certification. Plaintiff reserves the right to modify these class definitions as discovery in this action progresses.

61. Excluded from the Class are Defendants and their affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

62. **Numerosity**: While the precise number of class members has not yet been determined, members of the Classes are so numerous that their individual joinder is impracticable, as the proposed Classes appear to include many thousands of members who are geographically dispersed.

63. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all Class Members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the class members he seeks to represent. Accordingly, Plaintiff's claims are typical of Class Members' claims.

64. **Adequacy**: Plaintiff's interests are aligned with the Classes he seeks to represent and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and his counsel intend to prosecute this action vigorously. The Classes' interests are well-represented by Plaintiff and undersigned counsel.

65. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other class members' claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Defendants' wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

66. **Commonality and Predominance:** The following questions common to all class

members predominate over any potential questions affecting individual class members:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants' data security practices and the vulnerabilities of GEICO's systems resulted in the disclosure of Plaintiff's and other class members' sensitive information;
- whether Defendants violated privacy rights and invaded Plaintiff's and class members' privacy;
- whether Defendants were negligent or negligent per se in failing to protect sensitive information of Plaintiff and other class members;
- whether Defendants breached implied contracts with Plaintiff and class members;
- whether Defendants violated the New York GBL by failing to protect Plaintiff's and other class members' sensitive information, and permitting the Data Breach to occur; and
- whether Plaintiff and class members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

67. Given that Defendants engaged in a common course of conduct as to Plaintiff and the Classes, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, the New York Class)

68. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

69. Plaintiff brings this cause of action individually and on behalf of the Nationwide

Class or, in the alternative, the New York Class.

70. GEICO required Plaintiff and class members to submit non-public personal information as part of its regular business practices.

71. Defendants were entrusted with, stored, and otherwise had access to the personal information of Plaintiff and class members.

72. Defendants knew, or should have known, of the risks inherent to storing the personal information of Plaintiff and class members, and to not ensuring that GEICO's system were secure.

73. By collecting and storing this data, GEICO had a duty of care to use reasonable means to secure and safeguard this personal information, to prevent disclosure of the information, and to guard the information from theft. GEICO's duty included a responsibility to implement a process by which it could detect a breach of its systems in a reasonably expeditious period of time and to give prompt notice in the case of a data breach.

74. GEICO owed a duty to Plaintiff and class members to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that its systems and networks—and the personnel responsible for them—adequately protected its customers' personal information.

75. GEICO further assumed the duty to implement reasonable security measures as a result of its general conduct, internal policies and procedures, in which GEICO states, among other things, that GEICO.com's "[p]hysical safeguards, procedural controls and data access controls protect your data from unauthorized access" and GEICO "continually monitor[s] our systems to prevent unauthorized attempts at intrusion." Through these statements, GEICO specifically assumed the duty to comply with industry standards in protecting its customers' personal information.

76. GEICO's duty to use reasonable security measures arose from the special relationship existing between it and the Plaintiff and class members. The special relationship arose because Plaintiff and class members entrusted GEICO with their personal information, as

part of the insurance process. Only GEICO was in a position to ensure that its systems were sufficient to protect against harm to Plaintiff and the Class resulting from a data breach.

77. Defendants breached their duties to Plaintiff and class members, and thus was negligent, by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and class members' personal information, failing to adequately monitor the security of GEICO's online payment system and website, allowing unauthorized access to Plaintiff's and class members' personal information, failing to recognize in a timely manner that Plaintiff's and class members' personal information had been compromised, and failing to warn Plaintiff and class members in a timely manner that their personal information had been compromised.

78. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and class members, Plaintiff and class members would not have been injured.

79. Defendants acted with wanton disregard for the security of Plaintiff's and class members' personal information.

80. The injury and harm suffered by Plaintiff and class members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known they were failing to meet their duties, and that Defendants' breach would cause Plaintiff and class members to experience the foreseeable harms associated with the exposure of their personal information.

81. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and class members now face an increased risk of future harm.

82. Plaintiff and class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class,
or in the alternative, the New York Class)

83. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

84. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the New York Class.

85. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), GEICO had a duty to provide adequate data security practices in connection with safeguarding Plaintiff's and class members' personal information.

86. Defendants breached their duties to Plaintiff and class members under the Federal Trade Commission Act (15 U.S.C. § 45) and N.Y. Gen. Bus. Law § 349, among other statutes, by failing to provide fair, reasonable, or adequate data security in connection with the sale of insurance policies and use of the GEICO website in order to safeguard Plaintiff's class members' personal information.

87. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

88. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and class members, Plaintiff and class members would not have been injured.

89. The injury and harm suffered by Plaintiff and class members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiff and class members to experience the foreseeable harms associated with the exposure of their Personal Information.

90. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and class members now face an increased risk of future harm. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class,
or in the alternative, the New York Class)

91. Plaintiff realleges and incorporates all previous allegations as though fully set forth

herein.

92. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the New York Class.

93. Defendants required prospective clients and other consumers to provide their personal information in connection with the sale of insurance policies and the use of GEICO's online sale system, and as part of their regular business practices.

94. In connection with using the GEICO website or purchasing insurance policies from GEICO, Plaintiff and class members entered into implied contracts with GEICO.

95. Pursuant to these implied contracts, Plaintiff and class members provided GEICO with their personal information. In exchange, GEICO agreed, among other things: (1) to provide insurance services to Plaintiff and class members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and class members' personal information; and (3) to protect Plaintiff's and class members' personal information in compliance with federal and state laws and regulations and industry standards.

96. The protection of personal information was a material term of the implied contracts between Plaintiff and class members, on the one hand, and GEICO, on the other hand. Had Plaintiff and class members known that GEICO would not adequately protect its customers' and other consumers' personal information they would not have provided their personal information to GEICO.

97. Plaintiff and class members performed their obligations under the implied contract when they provided GEICO with their personal information.

98. Necessarily implicit in the agreements between Plaintiff/class members and GEICO was GEICO's obligation to take reasonable steps to secure and safeguard Plaintiff's and class members' personal information.

99. GEICO breached its obligations under its implied contracts with Plaintiff and class members by failing to implement and maintain reasonable security measures to protect their personal information.

100. GEICO's breach of its obligations of inherent to its implied contracts with Plaintiff and class members, i.e., its obligations to utilize adequate data security and privacy measures, directly resulted in the Data Breach.

101. The damages sustained by Plaintiff and class members as described above were the direct and proximate result of GEICO's material breaches of its agreements.

102. Plaintiff and other class members were damaged by GEICO's breach of implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their personal information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their personal information has been breached; (v) they were deprived of the value of their personal information, for which there is a well-established national and international market; (vi) they have suffered actual misuse of their personal information, and resulting fraud and identity theft; and/or (vii) they have lost time and money in connection with attempts to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT IV
Violations of New York General Business Law
N.Y. Gen. Bus. Law § 349 ("GBL")
(On Behalf of Plaintiff and the New York Class)

103. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

104. Plaintiff brings this cause of action on behalf of the New York Class.

105. Section 349 of the New York GBL provides that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful." N.Y. Gen. Bus. Law § 349(a).

106. Defendants, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade and commerce, and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the following:

a. failing to enact adequate privacy and security measures to protect Plaintiff's and class members' personal information from unauthorized disclosure, release, data breaches, and theft;

b. failing to take proper action following known security risks and prior cybersecurity incidents;

c. knowingly and fraudulently misrepresenting that Defendants would maintain adequate data privacy and security practices and procedures to safeguard personal information from unauthorized disclosure, release, data breaches, and theft;

d. omitting, suppressing, and concealing the inadequacy of Defendants' security protections;

e. knowingly and fraudulently misrepresenting that Defendants would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of personal information, and

f. failing to disclose the Data Breach to the victims in a timely and accurate manner, in violation of the duties imposed by, *inter alia*, N.Y. Gen Bus. Law § 899-aa(2).

107. As a direct and proximate result of Defendants' practices, Plaintiff and other class members suffered injury and/or damages, including but not limited to actual misuse of their personal information, fraud, and identity theft; lost time and expenses related to monitoring their accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their personal information.

108. The above unfair and deceptive acts and practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and other class members that they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

109. Defendants knew or should have known that GEICO's systems and data security practices were inadequate to safeguard personal information entrusted to it, and that risk of a data

breach was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

110. Plaintiff seeks relief under N.Y. Gen. Bus. Law § 349(h), including but not limited to actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

111. Plaintiff and class members seek to enjoin such unlawful deceptive acts and practices described above. Each class member will be irreparably harmed unless the Court enjoins Defendants' unlawful, deceptive actions in that Defendants will continue to fail to protect personal information entrusted to them, as detailed herein.

112. Plaintiff and class members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendants from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

COUNT V
Invasion of Privacy (Intrusion Upon Seclusion)
(On Behalf of Plaintiff and the Nationwide Class)

113. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

114. Plaintiff and class members had a reasonable expectation of privacy in the personal information that Defendants disclosed without authorization.

115. By failing to keep Plaintiff's and class members' personal information safe, knowingly utilizing unsecure systems, and disclosing personal information to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiff's and class members' privacy by, *inter alia*:

a. intruding into Plaintiff's and class members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. invading Plaintiff's and class members' privacy by improperly using their

personal information properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

c. failing to adequately secure their personal information from disclosure to unauthorized persons;

d. enabling the disclosure of Plaintiff's and class members' personal information without consent.

116. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and class members' position would consider its actions highly offensive.

117. Defendants knew that GEICO's systems were vulnerable to data breaches prior to the Data Breach.

118. Defendants invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and class members' private affairs by disclosing their personal information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

119. As a proximate result of such unauthorized disclosures, Plaintiff's and class members' reasonable expectations of privacy in their personal information was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiff's and class members' protected privacy interests.

120. In failing to protect Plaintiff's and class members' personal information, and in disclosing Plaintiff's and class members' personal information, Defendants acted with malice and oppression and in conscious disregard of Plaintiff's and class members' rights to have such information kept confidential and private.

121. Plaintiff seeks injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Classes, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as the class representative and undersigned counsel as class counsel;

B. Award Plaintiff and class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiff and class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and Class Members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: May 6, 2021

Respectfully submitted,

/s/ Tina Wolfson

TINA WOLFSON
twolfson@ahdootwolfson.com
ROBERT R. AHDOOT*
rahdoot@ahdootwolfson.com
CHRISTOPHER STINER
cstiner@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Ave., Suite 500
Burbank, CA 91505
Tel: 310-474-9111
Fax: 310-474-8585

ANDREW W. FERICH*
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC

201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

**pro hac vice* to be filed

Attorneys for Plaintiff and the Proposed Classes